Our Ref./Docket No.: CISCO-6592

A METHOD, APPARATUS, AND SOFTWARE PRODUCT FOR DETECTING ROGUE ACCESS POINTS IN A WIRELESS NETWORK

Inventor(s):

OLSON, Timothy S.
San Jose, California, USA

KAISER, Daryl A.
Los Gatos, CA, USA

ROSHAN, Pejman D.
Anaheim, CA, USA

Certificate of Mailing under 37 CFR 1.10

I hereby certify that this application and all attachments are being deposited with the United States Postal Service as Express Mail (Express Mail Label: EV325162838US in an envelope addressed to Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on.

Date: Jan. 28, 2004 Signed: John Nishinaga

Name: John Nishinaga

A METHOD, APPARATUS, AND SOFTWARE PRODUCT FOR DETECTING ROGUE ACCESS POINTS IN A WIRELESS NETWORK

RELATED PATENT APPLICATIONS

[0001] This invention claims the benefit of U.S. Provisional Patent Application Serial No. 60/490,847 S/N titled "A METHOD, APPARATUS, AND SOFTWARE PRODUCT FOR DETECTING ROGUE ACCESS POINTS IN A WIRELESS NETWORK" to inventors Tolson, et al., Docket/Reference No. CISCO-8125P, assigned to the assignee of the present invention, and incorporated herein by reference.

[0002] This invention is related to pending U.S. Patent Application Serial No. 10/629,384 titled "RADIOLOCATION USING A PATH LOSS DATA" to inventors Kaiser, et al., Docket/Reference No. CISCO-7391, assigned to the assignee of the present invention, and incorporated herein by reference.

BACKGROUND

[0003] The present invention is related to wireless networks, and in particular to network security and detecting rogue access points in an infrastructure wireless network.

[0004] Use of wireless networks such as wireless local area networks (WLANs) is becoming widespread. Furthermore, network security is becoming more and more important. Wireless networks present important network security concerns. One such concern is detecting rogue wireless stations.

[0005] A WLAN may be ad hoc, in that any station may communicate directly with any other station, or have an infrastructure in which a station can only communicate with another station via an access point (AP). The access point is typically coupled to other networks that may be wired or wireless, e.g., to the Internet or to an intranet. That wider network is called the "wired" network herein, and it is to be understood that this wired network may be an internetwork that include other wireless networks.

[0006] One aspect of the present invention addresses detecting rogue APs. We are mostly concerned with two types of rogue APs:

[0007] • An AP that is connected to a wired network of interest, e.g., to an otherwise secure LAN without authorization, and that thus may present a security hole for the secure network.

[0008] • An AP that is not connected to the wired network of interest but is in the radio environment of a wireless network (WLAN) of interest. Such an AP, by accepting associations may interfere with the WLAN of interest, e.g., by hampering potential client stations ("clients") from accessing their wireless network.

[0009] A rogue AP may be a malicious or non-malicious rogue AP. A non-malicious AP, for example, is the AP of a user who sets up such an AP for personal use either connected to the wired network of interest not in the wireless network of interest, without intentionally thwarting detection. Such a user is likely to use out-of-the-box default configuration. Therefore, when used in the radio environment of a WLAN of interest, the SSID of such a non-malicious AP typically will not match the SSID of the WLAN of interest.

[0010] A malicious rogue AP is one set up by a user in order to gain access to a wired network of interest, e.g., a secure LAN. Such a malicious AP may spoof the MAC address of a legitimate AP. Such a malicious AP may further set parameters such as the power, channel, and SSID again to spoof those of a legitimate AP in order to minimize the likelihood of being detected.

[0011] WLANs suffer several potential problems because of rogue access points. A rogue access point when connected to a secure network may cause the network to become insecure if proper security measures have not been enabled on the access point. In a well-designed WLAN the access points typically have been and configured to provide a certain level of coverage and capacity. Rogue access points can cause degradation to such planned coverage and capacity by causing contention with a legitimate access point, by causing collisions with a legitimate access point, and even by possibly causing denial of service for a legitimate client station.

[0012] There therefore is a need in the art for methods of detecting rogue APs.

[0013] Prior art methods for detecting rogue access points include having clients report failed authentication attempts on other APs, or detecting failed authentication attempts by the APs themselves. For example, an authentication tattletale method is known for reporting rogue access points. See U.S. patent application S/N 09/917,122 titled "ROGUE AP DETECTION" to Halasz, et al., filed 27-Jul-2001, assigned to the assignee of the present invention. and incorporated herein by reference. Such a prior-art method typically includes configuring a station with the appropriate identifier of the WLAN —a service set identifier (SSID)—to make an authentication attempt. Only rogues that are in the proper location to the clients i.e., in radio contact for an attempt at authentication can be detected. This can result in a delayed detection or no detection at all.

[0014] Other prior art methods include using some type of sniffer device that can be carried in the WLAN coverage area. An operator periodically walks the WLAN coverage with the sniffer device making measurements to search for rogue APs. See, for example, "AiroPeek and Wireless Security: Identifying and Locating Rogue Access Points" from WildPackets, Inc., Walnut Creek, CA (version dated Sep. 11, 2002).

[0015] Also known is a sniffer technique that uses APs as sniffers. See, for example, the document "AirWave Rogue Access Point Detection," from AirWave Wireless, Inc., San Mateo, California (www.airwave.com). Such APs are managed from a central location by a management entity. Most of the time, such a managed AP acts as regular access point. When a rogue scan is being conducted, a management entity issues a command, e.g., an SNMP command to the managed AP, converting it into a wireless sniffer. The managed AP scans the airwaves within its coverage radius, looking for traffic on all channels. The AP then reports all data back to the management entity as a trace, and then returns to normal operation mode. The management entity analyzes the traces from managed APs and sentry devices, comparing the detected APs to its database of authentic, managed APs. Such a method, however requires the AP to cease normal operation.

[0016] Prior art techniques are known for detecting rogue APs that require having a connection, e.g., a wired connection to the rogue AP. However, because a rogue AP may be a

device installed at a neighboring location, detection methods that require a wired connection may not always succeed.

[0017] Thus there is a need for a detection method that does not necessarily require a client to be in the area and that does not need special client configuration and that does not need an AP to stop its normal operation.

SUMMARY

[0018] Disclosed herein are a method, apparatus, and software product for detecting rogue access points. The proposed method can automatically detect rogue APs very quickly and possibly provide a broad location indication.

[0019] In one embodiment, the method includes maintaining an AP database that includes information about managed access points (APs) and friendly APs, defined to be known APs that are in the neighborhood of the managed network or that are known to clients of managed APs, i.e., to managed clients, and that are known to not cause problems, e.g. interference, to the managed wireless network. The method further includes sending a scan request to one or more managed APs, including one or more of a request for the receiving managed AP to scan for beacons and probe responses and a request for the receiving managed AP to request its clients to scan for beacons and probe responses. The method further includes receiving reports from at least one of the receiving managed APs, a report including information on any beacon or probe response received that was sent by an AP. For each beacon or probe response on which information is received, the method analyzes the information received in the report about the AP that sent the beacon or probe response, the analyzing including ascertaining if the MAC address of the AP that sent the beacon or probe response matches a MAC address of an AP in the AP database to ascertain whether or not the AP is a potential rogue AP or a managed or friendly AP.

[0020] In another embodiment, a method implemented in an access point of a wireless network is described. The method includes receiving a scan request at the AP to scan for beacons and probe responses, the request received from a WLAN manager managing a set of managed APs and client stations of the managed APs. The WLAN's managing includes maintaining an AP database that contains information about managed APs and friendly APs

of the wireless network. The method of the AP includes one or both of listening for beacons and probe responses at the AP itself or sending a client request to one or more client stations associated with the AP to listen for beacons and probe responses. In the case that a client request was sent, the method includes receiving a client report from at least one of the client stations to which the client request was sent, the client report including information on any beacon or probe response received from a potential rogue AP. The method further includes sending a scan report to the WLAN manager including information on any beacon or probe response received from a potential rogue AP by the AP receiving the scan request or, in the case that a client request was sent, by any client stations from which a report was received. The information includes the MAC address of the potential rogue AP.

[0021] For each beacon or probe response on which information is received at the WLAN manager, the WLAN manager may analyze the information received in the report about the potential rogue AP that sent the beacon or probe response, including ascertaining whether the MAC address of the potential rogue AP matches a MAC address of an AP in the AP database, leads to ascertaining whether or not the potential AP is likely to be a rogue AP.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] FIG. 1 shows a simple network that includes a WLAN manager on which one embodiment of the invention is implemented.

[0023] FIG. 2 shows the managed network of FIG. 1 with several rogue APs present, and illustrates the type of rogue APs that may be detected using embodiments of the invention.

[0024] FIG. 3 shows one embodiment of a wireless station 300 that may be an AP or a client station and that implements one or more aspects of the invention.

[0025] FIG. 4 shows a flow chart that includes in detail of the steps setting up, requesting, and receiving reports of the scans according to an embodiment of the invention.

[0026] FIG. 5 is a flow chart that describes the case of a Measurement Request Message including a request to schedule a managed AP to instruct one or more clients to perform scanning and report the results, according to an embodiment of the invention.

[0027] FIG. 6 shows the messaging and tasking at each entity of a simple example network.

[0028] FIG. 7 shows a flow chart of one embodiment of a method of detecting rogue access points.

DETAILED DESCRIPTION

[0029] Described herein is a method for detecting rogue access points, including malicious and non-malicious access points. The invention will be described in the context of the IEEE 802.11 standard for WLANs. The invention, however, is not restricted to WLANs that conform to the IEEE 802.11 standard.

The Managed Wireless Network

[0030] One embodiment of the invention operates in a managed wireless network in which the APs and their clients are managed by a central management entity. Depending on the size and complexity, a managed network is either a set of APs with a central control entity, or a hierarchical structure with a set of hierarchical control domains. Each control domain is managed by a management entity we call a manager herein. The number of levels in the hierarchy depends on the complexity and/or size of the network, and thus not all managed networks have all levels of control. For example, a simple managed network may only have one level of control with a single management entity controlling all the APs. Factors that influenced the selection of control domains include one or more of: the various types of IP subnet configurations; the radio proximity of the access points; the client station roaming patterns; the real time roaming requirements; and the physical constraints of the network (e.g. campus, building, and so forth.).

[0031] For example, one set of hierarchical domains includes a ***WLAN Campus Control Domain*** that is a region of integrated control over radio, mobility, QoS, and security aspects of a WLAN. Generally, a Campus Control Domain spans an enterprise campus that resides in a particular geographic location. Note that it is possible to have a higher-level network control entity join multiple Campus Control Domains together. As a WLAN expands it can grow large enough that a single control entity is unable to handle the intelligent control for all the APs in the campus. In such a case, the WLAN Campus Control Domain may be

segmented into ***WLAN Local Control Domains,*** each providing a subset of the functionality that is seen in the WLAN Campus Control Domain. A WLAN Local Control Domain, for example, may span a single building.

[0032] A WLAN Local Control Domain may contain one or more ***Subnet Control Domains***. The Subnet Control Domain contains all the APs within a single IP subnet or native virtual LAN (VLAN). Note that if no WLAN Local Control Domains exist, then the Subnet Control Domains would only be contained within the WLAN Campus Control Domain.

[0033] The domains are managed by one or more management entities we call ***managers***. Because of the hierarchical nature of the control domains, the associated managers are also naturally connected in a hierarchical manner. Thus, in the example above, a controller we call the ***Campus Context Manager***, also called the ***WLAN Manager*** is the highest point of context control in the hierarchy. The WLAN Manager manages several aspects of the wireless network, e.g., security, and in one embodiment, authorizes a set of access points in the network—we call these the ***managed access points***—including maintaining an AP database that includes the managed APs, e.g., a list of the managed APs together with some data related to these APs. The AP database also includes information about other APs the WLAN manager knows about. The WLAN Manager also managed the rogue AP detection aspects of the present invention. A single WLAN Manager is typically deployed to handle all the wireless clients within the enterprise campus.

[0034] If a given WLAN is segmented into multiple Local Control Domains, managers we call the ***Local Context Managers*** provide the next point of context control in the WLAN hierarchy, just below the WLAN Manager. A Local Context Manager manages client context information within each of these Local Control Domains and provides nearly all the same functionality as a WLAN Manager.

[0035] Within the WLAN Local Control Domain there are various control managers that handle different aspects of the WLAN such as QoS, client context transfer and radio management. The present invention is concerned with radio management.

[0036] If no Local Control Domains exist, then the other control managers would essentially operate at the same level as the WLAN Manager.

[0037] A controller we call the ***Subnet Context Manager*** provides the lowest level of context control within the WLAN hierarchy. One Subnet Context Manager is used within each subnet (or native VLAN) to coordinate client context transfer for roaming. The Subnet Context Manager manages client context transfer within the subnet. In one embodiment, Mobile IP is supported without requiring any modification to clients. Working in conjunction with the APs, the Subnet Context Manager provides proxy-Mobile IP services, and transparently handles all Mobile IP signaling requirements on behalf of all clients within the subnet.

[0038] A controller we call the ***Radio Manager*** provides intelligent centralized control of various aspects of the radio environment within a given set of APs. A single Radio Manager handles the radio aspects of all the APs within a given WLAN Local Control Domain or the WLAN Campus Control Domain if no local control domains exist. The Radio Manager provides the ability to determine network wide radio parameters during initial network deployment and network expansion. The Radio Manager centrally coordinates all client and AP measurements, e.g., in order to detect rogue access points.

[0039] Aspects of the invention are implemented on the Radio Manager and use the measurements made under control or direction of the Radio Manager. However, the invention does not require there to be a separate Radio Manager entity. The functionality of the Radio Manager may be incorporated into any of the other entities, e.g., the Local Context Manager or WLAN Manager when there are no Local Control Domains. Furthermore, these entities may be combined with other functionalities, e.g., switching, routing, etc.

[0040] Other management entities may be included at the Local Control Domain or Campus Control Domain if there are no Local Control Domains, such as network management to provide standard device network management functionality for any of the Subnet Context Managers, Quality of Service (QoS) management, and so forth.

[0041] When a WLAN is managed, one or more aspects of the invention (and of WLAN management in general) use information that is stored in a persistent database we call the ***Configuration Database***. The Configuration Database is the repository that all the Subnet Context Managers may use to save any persistent data. In one configuration, a single Configuration Database exists within the WLAN Campus Control Domain. The

Configuration Database either coexists with the Campus Context Manager or an external database may be used. The ***Configuration Database*** also includes the AP database that includes information about the managed APs and other APs the WLAN manager is aware of.

[0042] The invention is explained herein with reference to a simple network shown in FIG. 1. The network is not divided into Local Control Domains. All managers are assumed incorporated into a single management entity—a WLAN Manager 103—that has access to the Configuration Database. It is to be understood that the WLAN Manager incorporates the functions of the Radio Manager. In one embodiment, the WLAN substantially conforms to the IEEE 802.11 standard. By substantially conforming we mean compatible with. Some aspects of the IEEE 802.11 standard are modified slightly to accommodate some management aspects used in the invention. Furthermore, stations of the network measure the received signal strength relatively accurately.

[0043] In one embodiment, each of the wireless network management entities described above is implemented as software running under a network operating system such as IOS (Cisco Systems, Inc., San Jose California) on a processing system that includes one or more processors and that also carries out other network functions. Thus, the WLAN Manager, including aspects of the invention, may be implemented on a network switch or on a router. Similarly, the Subnet Context Manager may be implemented on a network switch or on a router.

[0044] In FIG. 1, the WLAN manager 103 is shown including a processing system 123 that includes one or more processors and a memory 121. The memory 121 includes instructions that cause one or more processors of the processing system 123 to implement the aspects of the present invention that are implemented in the WLAN Manager. The WLAN manager includes a network interface 125 for coupling to a network, typically wired. In one embodiment, the WLAN manager 103 is part of a network switch.

[0045] The WLAN Manager 103 is coupled via its network interface 125 and a network (typically a wired network) to a set of Subnet Context Managers. One such Subnet Context Manager is shown as element 105 in FIG. 1. All managed APs in a subnet register with a Subnet Context Manager. For example, in FIG. 1, the APs named AP1 and AP2 (107 and

109, respectively) each are part of the same subnet and have a network connection to Subnet Context Manager 105. Any management communication between the WLAN Manager 103 and APs 107 and 109 is then via the Subnet Context Manager 105.

[0046] A client station associates with an AP. Thus, in FIG. 1, APs 107 and 109 each are shown with associated clients 113, 115, and 117, 119, respectively. By a ***managed client*** we mean a client that associates with a managed AP. A ***managed wireless station*** is thus either a managed AP or a managed client. Thus, clients 113, 115, 117, and 119 are managed clients.

[0047] FIG. 2 shows the managed network of FIG. 1 with several rogue APs present, and illustrates the type of rogue APs that may be detected using embodiments of the invention. The managed APs 107 and 109 have approximate limits of their respective radio ranges shown by dotted lines 217 and 219, respectively. By way of example, a malicious AP is shown as AP3 203 having a limit of radio range 223. Two non-malicious rogues are shown as AP4 and AP6 with reference numerals 205 and 209, respectively, and approximate limits of radio range 225 and 229, respectively. Another non-managed AP is shown as AP5 207 having an approximate limit of radio range shown as 227. In this example, suppose AP5 is at a café frequented by a managed client of managed AP 107. Thus, the rogue AP3 203 is in radio range with client 119 of managed AP2 109. Similarly, the rogue AP4 203 is in radio range with client 115 of managed AP1 107. The rogue AP6 209 is in range of the managed AP1 107. The managed client 113 is in radio range of AP5 while not in radio range of its normal managed AP 107, and later returns to the radio range of its managed AP 107.

Radio Measurement

[0048] A wireless network uses management frames at the MAC layer designed, sent, and received for management purposes. For example, in a WLAN that conforms to the IEEE 802.11 standard, an AP regularly transmits beacon frames that announce the AP's presence, i.e., advertises the AP's services to potential clients so that a client may associate with the AP. Similarly, a client can send a probe request frame requesting any AP in its radio range to respond with a probe response frame that, in a similar manner to a beacon frame, provides information for the requesting client (and any other radios in its radio range and able to receive its channel) sufficient for a client to decide whether or not to associate with the AP.

[0049] Aspects of the invention use data from and/or about beacons and probe responses received at APs and/or client stations. The obtaining and receiving of such data is managed by the WLAN Manager 103.

[0050] By ***passive scanning***, we mean listening for beacons and probe responses without first transmitting a probe request. Thus, for an AP, passive scanning is the listening for and recording of information from beacons and probe responses from other APs that are transmitting such beacons and probe responses. For a client, passive scanning is the listening for and recording of information from beacons and probe responses from APs other than the clients AP that are transmitting such beacons and probe responses.

[0051] The use of passive scanning is an important aspect of the invention because it provides for rogue detection concurrent with normal processing at the station, e.g., at the AP.

[0052] By ***active scanning***, we mean transmitting a probe request prior to listening for beacons and probe responses. Both active and passive scanning can occur on the same channel used for wireless communication (the "serving" channel) or other channels ("non-serving" channels). For non-serving channels typically an active scan is used. One method we call ***incremental active scanning*** wherein the station probes another channel. Another we call ***full active scanning*** wherein the serving channel is vacated to probe all channels. Most wireless network interface devices support a mode usually called monitor mode wherein traffic on all channels is recorded, and this can be used for full active scanning.

[0053] FIG. 3 shows one embodiment of a wireless station 300 that may be an AP or a client station and that implements one or more aspects of the invention. While a wireless station such as station 300 is generally prior art, a wireless station that includes aspects of the present invention, e.g., in the form of software, is not necessarily prior art. The radio part 301 includes one or more antennas 303 that are coupled to a radio transceiver 305 including an analog RF part and a digital modem. The radio part thus implements the physical layer (the PHY). The digital modem of PHY 301 is coupled to a MAC processor 307 that implements the MAC processing of the station. The MAC processor 307 is connected via one or more busses, shown symbolically as a single bus subsystem 311, to a host processor 313. The host processor includes a memory subsystem, e.g., RAM and/or ROM connected to the host bus,

shown here as part of bus subsystem 311. Station 300 includes an interface 321 to a wired network.

[0054] In one embodiment, the MAC processing, e.g., the IEEE 802.11 MAC protocol is implemented totally at the MAC processor 307. The Processor 307 includes a memory that stores the instructions for the MAC processor 307 to implement the MAC processing, and in one embodiment, some or all of the additional processing used by the present invention. The memory is typically but not necessarily a ROM and the software is typically in the form of firmware.

[0055] The MAC processor is controlled by the host processor 313. In one embodiment, some of the MAC processing is implemented at the MAC processor 307, and some is implemented at the host. In such a case, the instructions for the host 313 to implement the host-implemented MAC processing are stored in the memory 315. In one embodiment, some or all of the additional processing used by the present invention is also implemented by the host. These instructions are shown as part 317 of memory.

[0056] According to one aspect of the invention, each station such as station 300 maintains a database of the beacons and probe responses it receives. Beacons and probe responses are stored in the database under one or more circumstances, e.g., when the station determines whether or not to associate with an AP. In the context of aspects of the present invention, beacons and probe responses received at the station are stored in the database as a result of an active scan or a passive scan. We call this database the Beacon Table. As shown in FIG. 3, in one embodiment, the Beacon Table 319 is in the memory 315 of the station. Other embodiments store the Beacon Table 319 outside of memory 315. A station stores the information in the beacons and probe responses in its Beacon Table 319, and further stores additional information about the state of the station when it receives the beacon.

[0057] According to an aspect of the invention, a station such as station 300 when implementing an AP is capable of passive scanning. According to yet another aspect of the invention, a station such as station 300 when implementing a client station is capable of passive scanning.

[0058] Because the station stores beacons and probe responses it has received in its Beacon Table, one form of passive scanning includes simply reporting the accumulated contents of the station's Beacon Table. Note that an alternate embodiment may alternately include the station's listening for a specified period of time and reporting the incremental Beacon Table information for the specified period of time.

[0059] According to yet another aspect, a station such as station 300 when implementing an AP is capable of active scanning, in particular incremental active scanning. To carry out an incremental active scan, the AP vacates its serving channel and probes one or more channels by sending a probe request frame on that/those channel(s). The AP prevents client transmissions by scheduling a contention free period (CFP). Alternatively the AP can prevent client transmissions by transmitting an unsolicited CTS with a duration long enough to cover the active scan time. According to yet another aspect, station 300 when implementing a client is capable of active scanning, in particular incremental active scanning. To carry out an incremental active scan, the client station vacates its serving channel and probes one or more channels by sending a probe request frame on that/those channel(s). In the case of a client, the active scan includes reporting back the results of probing the other channel(s). In order to prevent client transmissions from the serving AP the client must indicate that it is in a power save mode. Alternatively the client can use specific local knowledge such as application operation to assure that the AP will not send any transmissions directed at the client.

[0060] Scanning includes storing the information from beacons and probe responses received at the station, e.g., by passive or active scanning in the Beacon Table.

Radio Management Tasks and Communication Protocols

[0061] Aspects of the invention use radio measurement in managed APs and their clients, in particular as a result of passive and/or active scanning for beacons and probe responses. One embodiment uses a modified MAC protocol that adds transmission power control (TPC) and dynamic frequency selection (DFS). This may be a modification of the IEEE 802.11h standard. TPC limits the transmitted power to the minimum needed to reach the furthest user. DFS selects the radio channel at an AP to minimize interference with other systems, e.g., radar. Thus the IEEE 802.11h proposal provides for power control, channel scan, and

frequency selection. However, the inventors have found that 802.11's measurements decrease throughout. The IEEE 802.11h architecture (as of June 2003) uses a one-to-one request/response mechanism that may be inefficient.

[0062] Another embodiment, described in more detail herein, uses a protocol that differs from the presently proposed 802.11 protocol by providing for tasking at the AP and, in turn, at a client to autonomously carry out passive and/or active scanning for beacons and probe responses according to a schedule.

[0063] In one embodiment, the information reported includes, for each detected AP information about the detection, and information about or obtained from contents of the beacon/probe response. The detection information includes one or more of:

[0064] • The detected AP's BSSID, e.g., in the form of a MAC address.

[0065] • The channel the AP's probe response was received on.

[0066] • The MAC address of the receiving station.

[0067] • The RSSI detected at the PHY of the receiver of the beacon/probe response.

[0068] • Any other measures of received signal quality of the received beacon/probe response available at the PHY of the receiving station.

[0069] • Other received beacons. This may help locate the detecting station.

[0070] The beacon/probe response information sent includes one or more of:

[0071] • The SSID in the beacon or probe response.

[0072] • Beacon time (TSF timer) information. In one embodiment, this is sent in the form of TSF offset determined by comparing the timestamp in the beacon/probe response with the TSF timer at the managed AP receiving the response or at the managed client receiving the response.

[0073] • Configuration parameters included in the received beacon/probe response.

[0074] Note that some of this information is beyond what is presently (June 2003) proposed for IEEE 802.11h. Further note that while the IEEE 802.11 standard specifies that a relative RSSI value be determined at the physical level (the PHY), one aspect of the invention uses the fact that many modern radios include a PHY that provides relatively accurate absolute RSSI measurements. Thus, the reports include the RSSI detected at the PHY of the receiver of the received beacon/probe response. In one embodiment, RSSIs detected at the PHYs are used to determine location information from path loss.

[0075] One embodiment uses a protocol we call the ***WLAN Manager-to-AP Measurement Protocol*** to set up the passive and/or active scanning and communicate reports thereof. According to this protocol, the WLAN Manager can send a message we call a ***Measurement Request Message*** to, and receives report messages we call ***Measurement Report Messages*** from one or more managed APs, either directly, or via one or more Subnet Context Managers. The messages are encapsulated in IP packets, e.g., in Ethernet frames or UDP/TCI/IP packets. In one embodiment, Ethernet is used between a Subnet Context Manager and an AP, while IP encapsulation is used for inter-subnet messages.

[0076] In the case that the Measurement Request Message is to a Subnet Context Manager, the Measurement Request Message includes a measurement request routing list where one or more APs may reside and the request message for such APs. A Subset Context Manager receiving a Measurement Request Message forwards the request message to each AP in the routing list in the form of individual Measurement Request Messages for each destination AP. Each Measurement Request Message to an AP includes a specification of what actions are to be taken, how, and when, and applies to the AP and in one embodiment, to one or more of the AP's clients. According to the Measurement Request Message, the AP schedules its own measurements. In one embodiment, the WLAN Manager-to-AP Measurement Protocol provides for requesting a stream of measurements of specified duration and recurring as a specified periodic rate. The WLAN Manager may request measurements to be performed serially or in parallel.

[0077] The AP receiving the Measurement Request Message schedules the actual measurements. In one embodiment, the AP receiving a Measurement Request Message

responds with a message we call a ***Measurement Request Acknowledgment Message***, while in another embodiment, no acknowledgement is used.

[0078] In the case that the Measurement Request Message includes a schedule for one or more clients, the AP translates the Measurement Request Message into a measurement request for each client. In one embodiment, the measurement communication between the APs and clients uses MAC frames that conform to a modification of the IEEE 802.11 standard MAC protocol we call the ***AP-to-client Measurement MAC Protocol*** herein.

[0079] An AP receiving a Measurement Request Message periodically sends a report message we call a ***Measurement Report Message*** herein that includes reports from each station performing a measurement. The report part for each station includes the type of station performing the measurement (AP, client, and so forth), the MAC of the measuring station, and the actual measurement data. In this invention, we are concerned with reports of beacons and probe responses received at a station, and such a report in one embodiment includes the received signal strength (RSSI), e.g., in dBm, the channel, the measurement duration, the BSSID, TSF information in the beacon/probe response, and of the station receiving the beacon/probe response, the beacon interval, the capability contained in the beacon, and one or more other items of information.

[0080] The Measurement Report Messages are sent directly to the WLAN manager if no Subnet Context Managers are involved. In the case a context manager is in the path to the WLAN manager, the Subnet Context Manager receives the Measurement Report Messages from a set of APs in its subnet, and aggregates these to form an aggregated report that includes the individual reports. The aggregated report is sent as a Measurement Report Message to the WLAN manager.

The AP-to-client Measurement MAC Protocol

[0081] The AP-to-client Measurement MAC Protocol includes standard the IEEE 802.11 standard frames that are modified to include additional information that may be used by one or more embodiments of the invention. Any standard type MAC frames that conform to the AP-to-client Measurement MAC Protocol include an indication of such conformity. For example, an association request frame includes an element that indicated whether or not the

station supports radio management including the ability to carry out and report the client measurements described herein. A beacon frame and a probe frame that conform to the AP-to-client Measurement MAC Protocol may include the transmit power of the AP transmitting the frame.

[0082] A frame we call the ***Measurement Request Frame*** from the AP requests an active or passive scan by a client at a scheduled scan time with a report at a scheduled reporting time. Another message from the client to the AP produces a report back to AP on schedule. The Measurement Request Frame includes an identifier to be used by a responding client, scheduling information indicate when the action is to take place, and a set of one or more measurement report elements. The measurement report elements include indications as to what sort of report is requested, for example the report from an active scan, the report from a passive scan, or the station's accumulated Beacon Table without any scan.

[0083] A frame we call the ***Measurement Report Frame*** from the client provides a report in response to a Measurement Request Frame. The Report frame includes the MAC address of the station providing the report, the identifier from the corresponding Measurement Request Frame, and one or more measurement elements. The measurement elements for the case of a beacon or probe response include one or more of the channel number, the duration over which the beacon/probe response was measured, the PHY type (DSS, 5 GHz OFDM, and so forth), the RSSI of the beacon/probe response, the parent TSF, e.g., all or some of the lower order bits of the serving AP's TSF at the time the client received the beacon or probe response, the TSF in the beacon/probe response, and one or more other elements that are in the received beacon/probe response frame.

[0084] *Rogue AP Detection Using Radio Measurements*

[0085] One embodiment of the rogue detection method uses information about beacons and probe responses received by APs and/or client stations that are managed by the WLAN manager 107. The method will be described by way of example using FIG. 6 that shows the tasks and messaging performed by the WLAN Manager 103, the Subnet Context Manager 105, the AP 107 in the subnet of Subnet Context Manager 105, and a client 115 of the AP 107.

Overall Method using Radio Measurements

[0086] FIG. 7 shows the basic steps of the method. In step 703, the WLAN Manager 107 maintains an AP database that includes information about the APs that it manages. The AP database also includes information about the managed APs and about known APs that are in the neighborhood of the managed network or that are known to clients of managed APs, i.e., to managed clients, and that are known to not cause problems, e.g. interference, to the managed wireless network. Such APs are called ***friendly APs***. One example of a friendly AP is an AP at a coffee shop where an employee of the enterprise often works using a computer that is a managed client and that associates with this friendly AP. The AP database also includes information about rogue APs. In one embodiment, the AP database is in the Configuration Database and is automatically updated from time to time.

[0087] The information stored in the AP database about an AP includes the information from any beacon or probe response frame from such an AP, and any 802.11 information about the AP. In one embodiment, the 802.11 information includes the maximum power, the frequencies, and other 802.11 parameters. In some embodiment, the information further may include location information. In some embodiment, the information for each AP may further include other fields, e.g., fields used for other aspects of wireless network management. For example, in a managed network, it may be that the radio settings of the AP are managed and thus the WLAN manager knows the radio settings for the AP. The location of the AP also may be known.

[0088] One aspect of the invention compared information obtained from scanning for beacons or probe responses to information in the AP database. The comparison is of information from managed APs and in one embodiment, the clients of the managed APs about beacons or probe responses received from a potential rogue AP with information stored in the AP database about managed APs, friendly APs, and known or suspected rogue APs.

[0089] In one embodiment, the maintaining of the AP database includes updating the information in the AP database from time to time. The updating is automatic, e.g., whenever new information is obtained on potential rogue APs or whenever AP configurations are changed.

[0090] Thus, in a step 707, the WLAN manager sends one or more requests to one or more managed APs to carry out scanning. In one embodiment, the scanning by the APs is passive scanning. In another embodiment, the scanning by the APs is active scanning of one or more channels where potential rogue APs could be transmitting. Because a rogue AP may be outside the radio range of any managed APs, but still in the range of one or more clients of managed APs, in one embodiment, the request to the managed APs includes an instruction to request such APs' clients to carry out scanning. In one embodiment, the scanning by the managed clients is passive scanning. In another embodiment, the scanning by the managed clients is active scanning of one or more channels where a potential rogue AP could be transmitting.

[0091] As a result of such request, in a step 707, the WLAN manager receives reports from the APs and their clients on any beacons and probe responses received in the scanning by the APs and/or clients.

[0092] In a step 709, the WLAN manager analyzes information obtained in the received reports about the APs that transmitted the received beacons or probe responses, the analyzing including comparing with information in the AP database. The analysis step is discussed in more detail below. In summary, step 709 is to determine whether or not the transmitting AP is in the AP database. The MAC address (the BSSID) of the AP that sent the response is used to search the AP database for a match. In one embodiment, the analysis includes comparing configuration information in the beacon/probe response with information stored in the AP database about the configuration of managed APs. In one embodiment, the analysis further includes using timing information. In one embodiment, the analysis further includes using known location information of managed APs together with the timing information to determine the approximate location of the potential rogue AP in order to further ascertain whether the AP is likely to be a rogue. The results of the analysis step 709 include a classification of each AP as a friendly AP or a potential rogue AP.

[0093] One embodiment further includes step 711 of attempting to locate the receiving stations receiving the beacon and/or probe responses in order to attempt locating the potential rogue AP(s) to further ascertain whether or not the AP is likely to be a rogue. One location

method uses the RSSI at the station receiving the beacon/probe reponse together with a calibrated path loss model of the environment providing path losses at various locations to/from managed stations at known locations. The method is described further below and in concurrently filed pending U.S. Patent Application Serial No. 10/629,384 titled "RADIOLOCATION USING PATH LOSS DATA" to inventors Kaiser, et al., Docket/Reference No. CISCO-7391, assigned to the assignee of the present invention, and incorporated herein by reference.

[0094] One embodiment further includes step 713 of combining the results of the analysis with the results of one or more complementary rogue AP detection techniques. One such complementary technique includes a client reporting to a serving AP a failed previous authentication attempt with an AP, for example including identifying the suspected AP by its MAC address. One implementation uses an IEEE 802.1X over IEEE 802.11 security system, according to which client and APs are placed in an authentication server database. When a client authenticates, a session key gets delivered to the client and the access point separately. A client detects a failed authentication when it cannot use the session key after it has authenticated with the authentication server. The client eventually associates with another, now managed AP, and reports the potential rogue AP via the managed AP, to the WLAN manager. Such a complementary method is described in pending U.S. patent application S/N 09/917,122, filed July, 27, 2001, titled "ROGUE AP DETECTION," to inventors Halasz, et al., assigned to the assignee of the present invention, and incorporated herein by reference.

[0095] Using the radio location, the wireless network administrator (the IT person responsible for WLAN management; a user of the WLAN manager) can attempt to physically locate the AP. After locating the AP the administrator can classify the AP as either rogue, managed or friendly and update the WLAN database with information about the AP, including its classification as rogue, managed or friendly. If a rogue AP, the network administrator can issue an alert.

[0096] In one embodiment, the set of criteria to determine whether or not the AP is friendly or a rogue is set by the wireless network administrator and stored in the Configuration Database.

Setting Up Scans and Receiving Reports

[0097] FIG. 4 shows a flow chart that includes in more detail steps 705 and 707 of setting up, requesting, and receiving reports of the scans. Refer also to FIG. 6 that shows the messaging and tasks at each entity. In a step 403, at the WLAN manager 103, the wireless network administrator sets up a set of scan parameters that describe how information is to be obtained about beacons and probe responses received by managed APs, and in one embodiment, managed clients. The set of scan parameters includes whether an active scan or passive scan or both active and passive scan, and if an active scan, the one or more channels for the active scan. The set of scan parameters further includes the scan interval, e.g., the schedule of how often scans are to be performed, and in one embodiment, for how long. The set of scan parameters further includes an indication of whether the APs, the managed clients, or both the APs and clients are to perform the scans.

[0098] In a step 405, the WLAN manager 103 sends one or more Measurement Request Messages to the APs that instruct the APs to perform the scans and/or request their respective clients to perform the scans in the case that the wireless network includes one or more Subnet Context Managers, as in FIG. 6, the method includes forming a Measurement Request Message for each Subnet Context Manager that includes information sufficient for the Subnet Context Manager to send Measurement Request Messages to its APs.

[0099] In a step 407, the Subnet Context Manager, e.g., Subnet Context Manager 105 receives the Measurement Request Message and from the data therein, forms individual Measurement Request Messages and sends the messages to the respective target APs.

[00100] In a step 409, a target AP, e.g., AP 107 receives the Measurement Request Message and as a result, sets up tasking according to the request. The tasking includes scheduling any scans to be performed by the AP itself, and also, in the case the tasking includes for scanning by one or more clients, scheduling scans to be performed by the clients by sending request frames to the appropriate clients, and then receiving report frames from the clients. In the case that the request includes the AP performing scans, step 409 includes the AP 407 carrying out any passive and/or active scans requested in the Measurement Request Message. Such

action is carried out according to the schedule in the Request Message, e.g. periodically at a scheduled interval, and so forth.

[00101] In a step 413, the AP sends out Measurement Report Messages periodically according to the schedule in the Measurement Request Message. The Measurement Report Messages include information on the beacons/probe responses received by the AP if the AP was requested to perform scanning and, if the AP was requested to instruct its clients to perform scanning, information on the beacons/probe responses received by the clients. Such information includes information from the beacon/probe response and information about the state of the station when receiving the beacon/probe response. Thus, as shown in FIG. 6, a single request message generates periodic reports from the AP 107.

[00102] In a step 413, each Subnet Context Manager, e.g., Subnet Context Manager 105 receives the Measurement Report Messages sent periodically by managed APs in its subset, e.g., AP 107 according to the schedule in the Measurement Request Message. The Subnet Context Manager 105 aggregates Measurement Report Messages into a single aggregated Measurement Report Message and sends the Measurement Report Message to the WLAN manager 103.

[00103] The WLAN Manager receives Measurement Report Messages from APs, e.g., directly or via Subnet Context Managers. This is step 707 described above.

[00104] FIG. 5 is a flow chart that describes the case of the Measurement Request Message including a request to schedule an AP to instruct one or more clients to perform scanning and report the results. The steps shown in FIG. 5 are carried out periodically according to the schedule of the Measurement Request Message. The scheduling is carried out by the AP, e.g., AP 107 of FIG. 6. Thus at a scheduled time, in a step 503, the AP sends a Measurement Request Frame to the client or clients, e.g., client 115. In a step 505, the client receives the Measurement Request Frame and according to the content of the request, carries out the requested task, e.g., carries out a passive scan, an active scan at one or more specified channels, and/or sends its accumulated Beacon Table. In a step 507, the station after carrying out any scanning requested, sends a Measurement Report Frame to its serving AP. In a step 509, the AP receives the Measurement Report Frames from all clients that were requested.

Analysis of Reports

[00105] Step 709 of analyzing the information obtained from scans is now discussed in more detail. The WLAN manager compares information received from scans about a particular AP, including the particular AP's beacon/probe response with information in the AP database. In one embodiment, the comparison searches the AP database for a match with the particular APs' BSSID. Such a comparison may lead to a match with information in the AP database and suggest, for example, that the particular AP is a managed AP. However, there is some likelihood that the particular AP is spoofing a managed AP. In one embodiment, the comparison includes one or more known AP parameters that are obtained, e.g., part or all of the IEEE 802.11 standard information normally stored in a beacon/probe response. In a managed network, some or all of the AP parameters may be set by or known to the WLAN manager and stored in the AP database. Such parameters include one or more of the maximum power settings, the frequency, and other standard 802.11 parameters, and may also include specific proprietary fields that are not part of the IEEE standard. A comparison of the parameters may further determine whether or not the particular AP is likely to be a rogue AP.

[00106] In one embodiment, analyzing the information received about a particular AP, including the beacon/probe response also includes analyzing timing information to compare with timing information that would be expected of a managed or friendly AP. The timing information analyzed is of beacon time (TSF timer) offset determined by comparing the timestamp in the beacon/probe response with the TSF timer at the managed AP receiving the response or at the managed client receiving the response. Such an analysis may lead to conclude that the AP is not a managed AP.

[00107] In one embodiment, analyzing the information received about a particular AP, including the AP's beacon/probe response includes using the RSSI level at the receiver of the beacon/probe response from the potential rogue AP. In the case the beacon/probe response was detected by a managed AP, the location of the managed AP would be known and used together with the received RSSI to approximately locate the potential probe. In the case the beacon/probe response was detected by a client of a managed AP, the timing information may lead the WLAN manager to infer some location information. For example, the timing

information may provide an indication of when the client detected the beacon/probe response in relation to the time the client associated with the managed AP whose location is known.

[00108] Thus, the RSSI together with location information of managed APs and clients are used to approximately determine the location of the potential rogue AP in order to further ascertain whether the AP is likely to be a rogue. For example, this may provide the location to the nearest floor of a building.

Locating the Potential Rogues

[00109] Once potential rogues are identified, and even approximately located, e.g., to the level of a floor of a building, or within radio range of an AP of known location, one aspect of the invention is further locating the potential rogues using received signal strength information. One location method uses the RSSI at the station receiving the beacon/probe response together with a calibrated path loss model of the environment providing path losses at various locations to/from managed stations at known locations. The method is summarized here and described in more detail in concurrently filed pending U.S. patent application S/N 10/629,384 titled "RADIOLOCATION USING PATH LOSS DATA" to inventors Kaiser, et al., Docket/Reference No. CISCO-7391, assigned to the assignee of the present invention, and incorporated herein by reference.

[00110] In the case that the beacons/probe responses are detected by a set of managed APs, the locating method includes accepting an ideal path loss model and calibrating the ideal path loss model using path loss measurements between the managed access points in a region of interest, e.g., the floor of the building. The path loss measurements include the WLAN manager obtaining the received signal strengths from each respective access point receiving probe responses/beacons, e.g., on the channel that the rogue transmissions were received, for signals received as a result of probe responses/beacon transmissions by each other access point. Each transmission by a respective access point is at a known respective transmit power. The calibrating determines a calibrated path loss model between the managed access points.

[00111] The locating method further includes measuring the path loss between the potential rogue access point and at least some of the managed access points. The measuring is by the beacon/probe response reporting described herein. The measuring includes measuring the

received signal strength at each of at least some of the access points of the wireless network resulting from transmission of a beacon/probe response from the potential rogue access point for each of a set of assumed transmit powers for the potential rogue access point. The method further includes determining the likely location or locations of the wireless station using the measured path loss and the calibrated path loss model for the set of assumed transmit powers.

[00112] In the case the beacon/probe responses are detected at one or more clients, the location of the clients is first determined using a client-locating variant of the radio location method. The client at an unknown location receives beacons/probe responses from managed access points in the area of interest. The beacon/probe responses are at known transmit powers. The path loss is measured for each transmitting access point using reports from the receiving client station at an unknown location. The likely location or locations of the client station is determined comparing the received path loss components with the calibrated path loss model.

[00113] Once the location of the clients receiving the beacons/probe responses from the potential rogue AP are estimated, the method proceeds as for the case of APs receiving the transmissions from the potential rogue, with the determined location used as the "known" location of the receiving clients.

[00114] In the location determining (of a client or a potential access point), one embodiment includes using an exclusive likelihood function to provide a likelihood component as a function of location for each station at a known or determined location detecting a beacon or probe response from the potential rogue AP. One embodiment further uses an exclusive likelihood function to provide a likelihood component as a function of location for each station at a known or determined location that fails to detect a beacon or probe response from the potential rogue AP. In the case of the failure to detect, the station that fails to detect is assumed to receive at a particular signal strength, e.g., the specified receive sensitivity of the receiver of the station. The overall likelihood is the product of the inclusive and exclusive likelihood components. This is determined for each of the set of assumed transmit powers.

[00115] While FIG. 1 shows a network that includes Subnet Context Managers for subnets, embodiments of the invention also operate in networks with no Subnet Context Managers,

and larger networks that are further divided into other control domains. In the case of a smaller network than in FIG. 1, the communication that in a network such as FIG. 1 is between subnet context manager and its APs is then carried out directly between the WLAN Manager and the APs.

[00116] While in one embodiment, each Measurement Request Frame received at a client station generates a single Measurement Report Frame. In alternate embodiments, the client station may carry out tasking, e.g., schedule scanning events.

[00117] It should be appreciated that although the invention has been described in the context of the IEEE 802.11 standard, the invention is not limited to such contexts and may be utilized in various other applications and systems, for example other WLAN standards and other wireless standards.

[00118] One embodiment of each of the methods described herein is in the form of a computer program that executes on a processing system, e.g., one or more processors that are part of a WLAN manager. Thus, as will be appreciated by those skilled in the art, embodiments of the present invention may be embodied as a method, an apparatus such as a special purpose apparatus, an apparatus such as a data processing system, or a carrier medium, e.g., a computer program product. The carrier medium carries one or more computer readable code segments for controlling a processing system to implement a method. Accordingly, aspects of the present invention may take the form of a method, an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. Furthermore, the present invention may take the form of carrier medium (e.g., a computer program product on a computer-readable storage medium) carrying computer-readable program code segments embodied in the medium. Any suitable computer-readable medium may be used including a magnetic storage device such as a diskette or a hard disk, or an optical storage device such as a CD-ROM.

[00119] It will be understood that the steps of methods discussed are performed in one embodiment by an appropriate processor (or processors) of a processing (i.e., computer) system executing instructions (code segments) stored in storage. It will also be understood that the invention is not limited to any particular implementation or programming technique

and that the invention may be implemented using any appropriate techniques for implementing the functionality described herein. The invention is not limited to any particular programming language or operating system.

[00120] Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases "in one embodiment" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner, as would be apparent to one of ordinary skill in the art from this disclosure, in one or more embodiments.

[00121] Similarly, it should be appreciated that in the above description of exemplary embodiments of the invention, various features of the invention are sometimes grouped together in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the claims following the Detailed Description are hereby expressly incorporated into this Detailed Description, with each claim standing on its own as a separate embodiment of this invention.

[00122] All publications, patents, and patent applications cited herein are hereby incorporated by reference.

[00123] Thus, while there has been described what is believed to be the preferred embodiments of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the spirit of the invention, and it is intended to claim all such changes and modifications as fall within the scope of the invention. For example, any formulas given above are merely representative of procedures that may be used. Functionality may be added or deleted from the block diagrams and operations may be interchanged among functional blocks. Steps may be added or deleted to methods described within the scope of the present invention.